

Application Number 09/907,230

Amendment responsive to final Office Action mailed June 6, 2006

RECEIVED
CENTRAL FAX CENTER**AMENDMENTS TO THE CLAIMS**

AUG 03 2006

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

Claim 1 (Currently amended): A method of preventing creation of unauthorized and accessible copies of a first medium comprising:

receiving input from a user;

receiving an access key from the first medium, wherein the access key facilitates access to digital content on the first medium and includes uncorrected data and associated error correction information, wherein the error correction information of the access key includes one or more errors; and

controlling access to the digital content on the medium based on the input and the uncorrected data, wherein controlling access to the digital content on the medium includes:

copying the digital content from the first medium to a second medium;

applying the error correction information to the uncorrected data to produce a second access key that is modified relative to the access key that facilitates access to the digital content on the first medium, wherein the modification of the second access key is due to the application of the error correction information to the uncorrected data; and

copying the second access key to the second medium, wherein the second access key renders the second medium inaccessible.

Claim 2 (Currently amended): The method of claim 1, wherein controlling access to the digital content on the first medium further comprises:

invoking a device driver of a storage device to read the uncorrected data from the first medium without modification from application of the error correction information; and

comparing the uncorrected data and the input.

Application Number 09/907,230

Amendment responsive to final Office Action mailed June 6, 2006

Claim 3 (Currently amended): The method of claim 1, wherein controlling access to the digital content on the first medium further includes installing a software application from the first medium onto a computing system.

Claim 4 (Currently amended): The method of claim 1, wherein controlling access to the digital content on the first medium further includes executing a software application from the medium.

Claim 5 (Canceled).

Claim 6 (Currently amended): The method of claim 1, wherein controlling access to the digital content on the first medium further includes producing an audio output based on content stored on the first medium.

Claim 7 (Canceled).

Claim 8 (Original): The method of claim 1, wherein the error correction information includes error correction information selected from an error correction code, a cyclic redundancy code, and a Cross Interleaved Reed-Solomon Code.

Claim 9 (Currently amended): The method of claim 1, wherein controlling access to the digital content on the first medium further comprises decrypting the digital content contained within the first medium based on the uncorrected data and the input.

Claim 10 (Original): The method of claim 9, wherein the digital content comprises at least one of a software application, audio data, or video data.

Claim 11 (Original): The method of claim 1, wherein receiving the access key includes decrypting the access key.

Claim 12 (Original): The method of claim 1, further including selecting the access key from a plurality of access keys, where each of the access keys includes data and associated error correction information having one or more errors.

Application Number 09/907,230

Amendment responsive to final Office Action mailed June 6, 2006

Claim 13 (Currently amended): The method of claim 12, where selecting the access key includes:

assigning a random number to the first medium, wherein the random number is uniquely associated with the first medium;

selecting the access key from the plurality of access keys based on the random number;

generating a hash value from the random number and the selected access key; and

decrypting content of the first medium using the hash value.

Claim 14 (Original): The method of claim 1, wherein the uncorrected data includes accurate error correction information for the uncorrected data.

Claim 15 (Currently amended): A computer-readable medium comprising instructions that prevent creation of unauthorized and accessible copies of a first digital medium, wherein the instructions cause a programmable processor to:

receive input from a user;

read an access key from the first digital medium, wherein the access key facilitates access to digital content on the first digital medium and includes uncorrected data and associated error correction information, wherein the error correction information of the access key includes one or more errors; and

control access to the digital content on the first digital medium based on the input and the uncorrected data, wherein the instructions control access to the digital content by:

copying the digital content from the first digital medium to a second digital medium;

applying the error correction information to the uncorrected data to produce a second access key that is modified relative to the access key that facilitates access to the digital content on the first medium, wherein the modification of the second access key is due to the application of the error correction information to the uncorrected data; and

copying the second access key to the second digital medium, wherein the second access key renders the second digital medium inaccessible.

Application Number 09/907,230

Amendment responsive to final Office Action mailed June 6, 2006

Claim 16 (Currently amended): The computer-readable medium of claim 15, wherein the instructions cause the processor to invoke a device driver of a storage device to read the uncorrected data from the first digital medium without modification based on the error correction information, and to compare the uncorrected data and the input.

Claim 17 (Currently amended): The computer-readable medium of claim 15, wherein the instructions cause the processor to install a software application from the first digital medium onto a computing system based on the input and the uncorrected data.

Claim 18 (Currently amended): The computer-readable medium of claim 15, wherein the instructions cause the processor to execute a software application from the first digital medium based on the input and the uncorrected data.

Claim 19 (Currently amended): The computer-readable medium of claim 15, wherein the instructions cause the processor to produce an audio output from content stored on the first digital medium based on the input and the uncorrected data.

Claim 20 (Original): The computer-readable medium of claim 15, wherein the error correction information includes error correction information selected from an error correction code, a cyclic redundancy code, and a Cross Interleaved Reed-Solomon Code.

Claim 21 (Currently amended): The computer-readable medium of claim 15, wherein the instructions cause the processor to decrypt the digital content from the first digital medium based on the uncorrected data.

Claim 22 (Original): The computer-readable medium of claim 15, wherein the uncorrected data includes accurate error correction information for the uncorrected data, and where the processor corrects errors in the uncorrected data with the accurate error correction information.

Application Number 09/907,230

Amendment responsive to final Office Action mailed June 6, 2006

Claim 23 (Currently amended): A first computer-readable medium comprising:

digital content;

an access key that facilitates access to the digital content on the first computer-readable medium and prevents creation of unauthorized copies of the first computer-readable medium, wherein the access key includes uncorrected data and associated error correction information having one or more errors;

an executable software application to control access to the digital content based on the uncorrected data by applying the error correction information to the uncorrected data to produce a second access key when the digital content is copied from the first computer-readable medium to a second computer-readable medium, wherein the second access key is modified relative to the access key that facilitates access to the digital content on the first computer-readable medium, wherein the modification of the second access key is due to the application of the error correction information to the uncorrected data, and wherein the second access key is copied to the second computer-readable medium as its respective access key thereby rendering the second computer-readable medium inaccessible.

Claim 24 (Currently amended): The first computer-readable medium data storage device of claim 23, wherein the digital content comprises a software program.

Claim 25 (Currently amended): The first computer-readable medium data storage device of claim 23, wherein the digital content is selected from one of an audio file and a video file.

Claim 26 (Currently amended): The first computer-readable medium data storage device of claim 23, wherein the error correction information includes an incorrect cyclic redundancy code.

Claim 27 (Currently amended): The first computer-readable medium data storage device of claim 23, wherein the error correction information causes the uncorrected data to be changed when the computer-readable medium is copied.

Application Number 09/907,230

Amendment responsive to final Office Action mailed June 6, 2006

Claim 28 (Currently amended): The first computer-readable medium data storage device of claim 23, wherein the uncorrected data includes accurate error correction information that corrects errors in the uncorrected data.

Claim 29 (Currently amended): A method of preventing creation of unauthorized and accessible copies of a first medium comprising:

generating an access key that facilitates access to digital content on the first medium, wherein the access key includes uncorrected data and incorrect error correction information;
associating the digital content and the access key on the first medium;
copying the digital content from the first medium to a second medium;
applying the error correction information to the uncorrected data to produce a second access key, wherein the second access key is modified relative to the access key that facilitates access to the digital content on the first medium, wherein the modification of the second access key is due to the application of the error correction information to the uncorrected data; and
copying the second access key to the second medium, wherein the second access key renders the second medium inaccessible.

Claim 30 (Previously presented): The method of claim 29, wherein associating the digital content and the access key comprises communicating the digital content and the access key through a transmission medium.

Claim 31 (Currently amended): The method of claim 29, wherein associating the digital content and the access key comprises storing the digital content and the access key on the first medium.

Claim 32 (Canceled).

Application Number 09/907,230

Amendment responsive to final Office Action mailed June 6, 2006

Claim 33 (Currently amended): The method of claim 29, further comprising:
receiving input from a user;
generating an encryption key based on the input and the access key that facilitates access to the digital content on the first medium;
encrypting the digital content based on the encryption key; and
associating the encrypted digital content with the access key that facilitates access to the digital content on the first medium.

Claim 34 (Currently amended): The method of claim 33, wherein associating the encrypted digital content with the access key that facilitates access to the digital content on the first medium comprises communicating the encrypted digital content and the access key that facilitates access to the digital content on the first medium through a transmission medium.

Claim 35 (Original): The method of claim 29, wherein the digital content includes an audio file.

Claim 36 (Original): The method of claim 29, wherein the digital content includes an application file.

Claim 37 (Original): The method of claim 29, wherein generating the access key includes generating uncorrected data having accurate error correction information.

Claim 38 (Currently amended): The method of claim 1, wherein the access key comprises a cryptographic access key that facilitates decryption of the digital content on the first medium.